ANTI-MONEY LAUNDERING/COUNTERING FINANCING OF TERRORISM POLICY & PROCEDURES

FIRST EQUITY MODARABA

1) Definition

The conversion or transfer of property, the concealment or disguising of the nature of the proceeds, the acquisition, possession or use of property, knowing that these are derived from criminal activity and participate or assist the movement of funds to make the proceeds appear legitimate is money laundering.

Money Laundering is the process by which, criminals attempt to make the proceeds of crime appear legitimate with no obvious links to their criminal origins. This is achieved by three processes:

i. Placement – Placing of the proceeds of crime
ii. Layering – Hiding of the proceeds from their criminal origin by 'layers' of transactions
iii. Integration – Creating a legitimate explanation for the proceeds

Anti-money laundering (AML) is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities.

Effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse

2) BACKGROUND AND INTRODUCTION

In the last few years, across the world regulations have been put in place to discourage money laundering and financing of illegal/criminal activities. Pakistan is a signatory to such agreement and is a member of relevant bodies such as Financial Action Task Force (FATF). In view of recommendations of FATF and other relevant bodies and implement appropriate policies and procedures. Pakistan has enacted the Anti Money Laundering Act 2010. In the above context, apex capital market regulator, the SECP have provided comprehensive guidelines for Pakistan financial institutions regarding how to develop and implement policies and procedures.

Anti-money-laundering and countering financing of terrorism refers to a set of procedures, laws and regulations designed to stop the practice of generating income through illegal actions. Though anti-money-laundering laws cover a relatively limited number of transactions and criminal behaviors, their implications are far-reaching. For example, AML regulations require institutions issuing credit or allowing customers to open accounts to complete due-diligence procedures to ensure they are not aiding in money-laundering activities. The onus to perform these procedures is on the institutions, not on the criminals or the government

An effective Anti-Money Laundering and Countering the Financing of Terrorism ("**AML/CFT**") regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF. AML and CFT Regime is governed under Anti-Money Laundering Act, 2010 ("**AML Act**"), Anti-Money

Laundering Rules, 2008 ("**AML Rules"**) made under the Anti-Money Laundering Ordinance, 2007 ("**AML Ordinance**"), Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations, 2018 ("**SECP AML/CFT Regulations"**) made under the Securities and Exchange Commission of Pakistan Act, 1997 (**"SECP Act"**), upon recommendation of Financial Monitoring Unit (**"FMU"**) established under AML Act, Guidelines on SECP AML/CFT Regulations issued by SECP in September 2018 and Pakistan National Risk Assessment (PNRA) Report on Money Laundering and Terrorist Financing issued in September 2019.

3) OBLIGATION IN ESTABLISHING AN EFFECTIVE AML/CFT REGIME

a) FEM understand its obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes, and to develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

b) Our Board of Directors and senior management is engaged in the developing and implement policies, procedures, controls and decision making on Money Laundering **(ML)** and Terrorist Financing **(TF)**. FEM is aware of the level of ML/TF risk that the Modaraba is exposed to and take a view on whether it is equipped to mitigate that risk effectively.

c) FEM is giving a due priority to establishing and maintaining an effective AML/CFT compliance culture and adequately train its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations.

d) To oversee the compliance function, FEM appointed a Compliance Officer ("CO") at the management level and a Head of Internal Auditor (HIA). HIA shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit (FMU).

e) FEM ensure that any suspicious transaction report must be made by employees to the Compliance Officer and/or HIA, who is well versed in the different types of transactions which FEM handles and which may give rise to opportunities.

f) FEM is responsible to ensuring that employees should be aware of their reporting obligations and the procedure to follow when making a suspicious transaction report.

4) PROCESS OF RISK ASSESSMENT.

FEM would performed risk assessment process in order to identify, assess and understand, ML/TF risks arising from customers; linkages to other countries via customers and operations dealing; products, services , transaction and delivery channels.

In risk assessment, we take into account all the relevant risk factors and categorize the overall risk as High Medium or low.

FEM will also follow the methodology for Internal Risk Assessment as required by PNRA Report. The concepts as defined by PNRA report, i.e. threat, vulnerabilities, inherent risk, consequences and likelihood of ML/TF and remedial measures / controls will be taken into consideration. The vulnerabilities will be assessed by considering the products and services offered, the customers, the geographical reach and delivery channels available.

FEM Management understand the nature and level of the risks that they are exposed to and ensure that systems and processes are in place to identify, assess, monitor, manage and mitigate ML/TF risks.

FEM will take appropriate steps to identify, assess and understand, its money laundering and terrorism financing risks in relation to-

(a) its customers;
(b) the jurisdictions or countries its customers are from or in;
(c) the jurisdictions or countries the FEM has operations or dealings in; and
(d) the products, services, transactions and delivery channels by FEM .

The appropriate steps referred above shall include-

(a) documenting the risk assessments;
(b) considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied;
(c) keeping the risk assessments up-to-date;
(d) categorizing the overall entity level risk as high, medium or low based on the result of risk assessment; and
(e) having appropriate mechanisms to provide its risk assessment information to the Commission.

5) RISK MITIGATION & APPLYING RISK BASED APPROACH

FEM have develop appropriate policies, procedures and controls that enable to manage and mitigate effectively the risks that have and can be identified. FEM would continuously monitor the implementation of controls and enhance them, if necessary.

The policies, controls and procedures are approved by the Board of Directors of the Modaraba management Company. Senior management will monitor the implementation of those policies, procedures and controls and will enhance and amendments them if necessary

CO/HIA will effectively manage and mitigate the risks that are identified in the risk assessment of ML/TF or notified by the Commission and will take measures to manage and mitigate the risks (whether higher Medium or lower) should be consistent with legal and regulatory requirements.

The nature and extent of our AML/CFT controls will depend on a number of aspects, which include:

1) The nature, scale and complexity of business
2) Diversity, including geographical diversity of the operations
3) Customer, product and activity profile
4) Volume and size of transactions

5) Extent of reliance or dealing through third parties or intermediaries.

Some of the risk mitigation measures that we consider include:

1) Determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers;
2) Setting transaction limits for higher-risk customers or products;
3) Requiring senior management approval for higher-risk transactions, including those involving PEPs;
4) Determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;
5) Determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

6) NEW PRODUCTS, PRACTICES AND TECHNOLOGIES.

(a) identify and assess the money laundering and terrorism financing risks that may arise in relation to-

   (i) the development of new products and new business practices, including new delivery mechanisms; and
   (ii) use of new or developing technologies for both new and pre-existing products;

(b) undertake the risk assessments, prior to the launch or use of such products, practices and technologies, and shall take appropriate measures to manage and mitigate the risks.

(c) in complying with the requirements of clauses (a) and (b), pay special attention to any new products and new business practices, including new delivery mechanisms; and new or developing technologies that favor anonymity.

7) DEFENSE MECHANISM

FEM established the following three lines of defense to combat ML/TF;

1) First the business units (e.g. front office, customer-facing activity): They should know and carry out the AML/CFT due diligence related policies and procedures and be allotted sufficient resources to do this effectively.

2) Second the Compliance Officer, the compliance function and human resources or technology.
3) Third the internal audit function

8) PERIODIC MONITORING OF AML/CFT SYSTEMS & CONTROLS

Once the identification procedures have been completed and the business relationship is established, it requires monitoring the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened.

FEM shall conduct ongoing monitoring of their business relationship with the customers. Ongoing monitoring helps to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

FEM would conduct on-going due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer.

Examples of triggering events include:

I. Material changes to the customer risk profile or changes to the way that the account usually operates;
II. Where it comes to the attention that it lacks sufficient or significant information on that particular customer;
III. Where a significant transaction takes place;
IV. Where there is a significant change in customer documentation standards; and
V. Significant changes in the business relationship.

There would be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

i. Transaction type
ii. Frequency
iii. Amount
iv. Geographical origin/destination
v. Account signatories

9) CUSTOMER DUE DILIGENCE & IDENTIFICATION PROCEDURES

i. FEM shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or may complete verification after the establishment of the business relationship and will not open or maintain anonymous account or an account in fictitious name.

ii. FEM will apply CDD measures when establishing business relationship with a customer and when there is doubt about the veracity or adequacy of previously obtained customer identification data.

iii. FEM Customer due diligence (CDD) will include among other things –

(a) identifying the customer or beneficial owner and verifying the customer's/beneficial owner's identity on the basis of documents, data or information obtained from customer and/or from reliable and independent sources;

(b) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

(c) monitoring of accounts/transactions on ongoing basis to ensure that the transactions being conducted are consistent with the knowledge of the customer, the customer's business and risk profile, including, the source of funds and, updating records and data/ information to take prompt action and when there is material departure from usual and expected activity through regular matching with information already available with FEM

iv. FEM will obtain such documents from different types of customers as required under the Regulation

v. FEM will verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or may complete verification after the establishment of the business relationship, provided that-

(a) this occurs as soon as reasonably practicable;
(b) this does not interrupt the normal conduct of business; and
(c) the ML/TF risks are effectively managed.

vi. FEM will adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification. The types of circumstances where FEM / Regulation permits completion of verification after the establishment of the business relationship should be recorded in their CDD policies.

vii. For all persons, FEM will determine whether the person is acting on behalf of a customer and should take reasonable steps to obtain-

(a) evidence to determine authority of such person to act on behalf of the customer, which shall be verified through documentary evidence including specimen signature of the customer;
(b) identification and verification of the person purporting to act on behalf of the customer;
(c) identification and verification of the customer;

viii. Each customer shall be categorized as high or low risk, depending upon the outcome of the CDD process;

ix. FEM will maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of negative verification;

x. FEM will apply CDD requirement to its existing customers on the basis of materiality and risk and should conduct due diligence on existing relations at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained;

xi. Where FEM is not able to satisfactorily complete required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR and where CDD of an existing customer is found unsatisfactory, the relationship should be treated as high risk and reporting of suspicious transaction under the Regulation;

xii. Where FEM forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it may not pursue the CDD process, and instead should file an STR in accordance with Regulation.

xiii. Government entities accounts will not be opened in the personal names of the government officials and account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity. It will only be opened on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government. FEM will also take into account any rules, regulations or procedures prescribed in the governing laws of such entities relating to opening and maintaining of their bank accounts.

9.1) ENHANCED DUE DILIGENCE

I. FEM will implement appropriate internal risk management systems, policies, procedures and controls to determine if any customer presents high risk of ML/TF.

II. For the purposes of sub-regulation (1), circumstances where a customer presents high risk of ML/TF include but are not limited to the following

(a) customers/ policy holders belonging to countries which are non-compliant with anti-money laundering regulations according to FATF;
(b) such body corporate, partnerships, associations and legal arrangements including non-governmental organizations or not-for-profit organizations which receive donations; and
(c) legal persons or arrangements with complex ownership structures.

III. FEM will ensure to have AML/CFT measures consistent with the requirements of Pakistan.

IV FEM shall perform EDD proportionate to risk posed to the business relationship by the customers that are identified as high risk or are notified as such by the Commission.

V. FEM will adopt risk management procedures with respect to the conditions under which an applicant may utilize the business relationship, prior to verification

VI EDD measures include but are not limited to the following-

a. obtain approval from Senior management to establish or continue business relations with such customers;
b. establish, by appropriate means, the sources of wealth and/or funds or beneficial ownership of funds, as appropriate; including regulated person' own assessment to this effect;
c. conduct during the course of business relations, enhanced monitoring of business relations with the customer
d. Obtain information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
e. Updating more regularly the identification data of applicant/customer and beneficial owner.
f. Obtain information on the intended nature of the business relationship.
g. Obtain information on the source of funds or source of wealth of the applicant/customer.
h. Obtain information on the reasons for intended or performed transactions.
i. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
j. Evaluating the country status of applicant/customer and its nominee and when anyone residing or was reside in any high risk country and/or area, in the first stance the account will not be opened and for further instruction the matter will be refer to management.

.

9.2) PROCEDURES FOR INDIVIDUALS

(a) For identifying the customer, the following information / documents will be obtained and the same will be recorded with Account Opening Forms at the Brokerage house :

i. Account Holder Name
ii. Mailing Address
iii. Permanent Address
iv. NTN No.
v. Jurisdiction of Residence
vi. Nationality
vii. Email Address
viii. Details of Bank Account
ix. Source of Income
x. Computerized National Identity Card No.

(b) **Documents**

Any one of the following valid identity will be required:

i. Computerized National Identity Card (CNIC) issued by NADRA
ii. National Identity Card for Overseas Pakistani (NICOP) issued by NADRA
iii. Pakistan Origin Card (POC) issued by NADRA

iv. Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only)
v. Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only)

9.3) PROCEDURE FOR PARTNERSHIP, TRUST, LIMITED COMPANIES CORPORATIONS, ANY OTHER LEGAL ENTITY

FEM will take all reasonable measures and satisfactory evidence of any entity to ensure the compliance of the Regulations.

(a) The following information will be obtained and the same will be recorded with Account Opening Forms at the Brokerage house:

Name of Company
i. Registration No.
ii. Date of Incorporation
iii. Business Commenced on
iv. Status
v. Type
vi. Email, Website
vii. Contact Numbers
viii. Mailing Address
ix. NTN Number
x. Contact Person
xi. Bank Account
xii. Expected Mode of Transactions

(b) Documents

i. Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account.
ii. Memorandum and Articles of Association
iii. Certificate of Incorporation
iv. Certificate of Commencement of Business, wherever applicable
v. List of Directors on Form-A / Form-B issued under Companies Act, 2017, as applicable and Form-29 where applicable
vi. Photocopies of identity documents for all the directors and persons authorized to open and operate the account.

10) TIMING OF VERIFICATION

FEM will undertake to verification, prior to entry into the business relationship or conducting a transaction.

11) MODE OF PAYMENT

All payments and receipt shall be through cross cheques, payorder, demand draft, negotiable instruments or any mode of banking channels. Where payment / receipt is made through cross cheque or etc, copy of the cheques or instrument will be retain.

We would ensure that amount in excess of Rs. 25,000/- will only be received from a customer, in exceptional circumstances, where it becomes necessary and such instances will be reported to the Stock Exchange.

12) BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND LEGAL ARRANGEMENTS.-

(i) Where the customer is a legal person, in addition to other measures following will ensure-

(a) understand the nature of the customer's business and its ownership and control structure;
(b) identify and verify the identity of the natural persons (whether acting alone or together) who ultimately own the legal person by obtaining relevant information from the customer as per Regulations;
(c) where there is doubt under clause (b) as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person; and
(d) where no natural persons are identified under clause (b) or (c), identify the natural persons having executive authority in the legal person, or in equivalent or similar positions.

(ii) Where the customer is a legal arrangement, the FEM will ensure-

(a) for trusts, identify and verify the identity of the settlor, the trustee, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristic or class), and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership); and
(b) for other types of legal arrangements, identify and verify the identity of persons in equivalent or similar positions, as those described under clause (a).

13) POLITICALLY EXPOSED PERSONS (PEPS)

FEM, in relation to PEPs, in addition to performing normal due diligence measures, shall ensure:

a) to have appropriate risk management systems to determine whether the customer is a politically exposed person

b) to obtain senior management approval for establishing business relationships with such customers
c) To take reasonable measures to establish the source of wealth and source of funds.
d) to conduct enhanced ongoing monitoring of the business relationship

In assessing the ML and TF risks of a PEP, FEM shall consider factors such as whether the customer who is a PEP:

a) is from a high risk country
b) has prominent public functions in sectors known to be exposed to corruption has business interests that can cause conflict of interests (with the position held)

The above criteria will also applicable on family members and close associates of foreign and domestic PEPs

14) SIMPLIFIED DUE DILIGENCE.-

(i) Where low risk is identified through adequate analysis of risk or where adequate checks and controls exist, FEM may apply simplified or reduced Customer Due Diligence / Know Your Customer measures.

(ii) The decision to rate a customer as low risk shall be justified in writing and low risk cases may include but are not limited to the following-

(a) provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements;
(b) public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership;
(c) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(iii) Subject to above, low risk for Simplified Due Diligence measures are limited to the following-

(a) Reducing the frequency of customer identification updates;
(b) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold; and
(c) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established:

Provided that Simplified CDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

15) RECORD KEEPING PROCEDURES

(i) Maintain all necessary records and transactions, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) for a minimum period of five years from completion of the transaction:

Provided that may retain those records for longer period where transactions, customers or accounts involve litigation or it is required by court or other competent authority.

(ii) The records shall be sufficient to permit reconstruction of individual transactions including the nature and date of the transaction, the type and amount of currency involved and the type and identifying number of any account involved in the transactions so as to provide, when necessary, evidence for prosecution of criminal activity and the transactions records may be maintained in paper or electronic form, provided it is admissible as evidence in a court of law.

(ii) The records of identification data obtained through CDD process like copies of identification documents, account opening forms, Know Your Customer forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of five years after termination of the business relationship

16) SUSPICIOUS TRANSACTIONS/CURRENCY TRANSACTION REPORT

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction is considered unusual, and should be put "on enquiry". Special attention should be pay to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose

Where the enquiries conducted by FEM do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML/CFT

Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, and made available to the relevant authorities upon request.

Activities which should require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

a. any unusual financial activity of the customer in the context of the customer's own usual activities;

b. any unusual transaction in the course of some usual financial activity;
c. any unusually-linked transactions;
d. any unusual method of settlement;
e. any unusual or disadvantageous early redemption of an investment product;
f. any unwillingness to provide the information requested.

Where cash transactions are being proposed by customers and such requests are not in accordance with the customer's known reasonable practice, need to approach such situations with caution and make further relevant enquiries.

Where unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. FEM will file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above

17) RELIANCE ON THIRD PARTIES.-

(i) FEM may rely on a third party to conduct CDD on its behalf provided that IT shall-

(a) obtain immediately, the necessary information relating to identification of business of the customer;

(b) take steps to satisfy that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

(c) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with the Regulations; and

(d) maintain data/ information confidentiality and non-disclosure agreement with the third party.

(ii) When determining in which countries the third party that meets the conditions can be based, FEM should have information available on the level of country risk.

(iii) When rely on a third party that is part of the same financial group:

(a) the group should apply CDD and record-keeping requirements and programmes against money laundering and terrorist financing, in accordance with these Regulations; and

(b) any higher country risk should be adequately mitigated by the group's AML/CFT policies.

(iv) FEM will be responsible for ongoing monitoring of its customers and notwithstanding the reliance upon a third party.

18) ONGOING MONITORING.-

(i) All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.

(ii) FEM will obtain information and examine, as far as possible the background and purpose of all complex and unusual transactions, which have no apparent economic or visible lawful purpose and the background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required.

(iii) Periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers and the review period and procedures thereof should be defined by FEM in their AML/CFT policies, as per risk based approach.

(iv) In relation to above, customers' profiles should be revised keeping in view the spirit of Know Your Customer/CDD and basis of revision shall be documented and customers may be consulted, if necessary.

(v) Where FEM files an STR on reasonable grounds for suspicion that existing business relations with a customer are connected with ML/TF and FEM may considers it appropriate to retain the customer-

(a) FEM shall substantiate and document the reasons for retaining the customer; and
(b) the customer's business relations with FEM shall be subject to proportionate risk mitigation measures, including enhanced ongoing monitoring.

(vi) FEM will not form business relationship with entities/individuals that are:

(a) Proscribed under the United Nations Security Council Resolutions and adopted by the Government of Pakistan;
(b) Proscribed under the Anti Terrorism Act, 1997(XXVII of 1997); and
(c) associates/facilitators of persons mentioned in (a) and (b).

(vii) FEM will monitor their relationships on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, FEM will take immediate action as per law, including freezing the funds and assets of such proscribed entity/individual and reporting to the Commission.

19) REPORTING OF TRANSACTIONS (STRS/CTRS).-

(i) FEM will comply with the provisions of the AML Act and rules, regulations and directives issued there under for reporting suspicious transactions/currency transactions in the context of money laundering or financing of terrorism.

(ii) FEM will implement appropriate internal policies, procedures and controls for meeting their obligations under the AML Act.

(iii) FEM will pay special attention to all complex and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions shall, as far as possible, be examined, the findings established in writing, and be available to assist the relevant authorities in inspection and investigation.

(iv) The transactions, which are out of character, are inconsistent with the history, pattern, or normal operation of the account or are not commensurate with the level of income of a customer shall be viewed with suspicion, be properly investigated and referred to Compliance Officer for possible reporting to FMU under the AML Act.

(v) FEM will note that STRs, including attempted transactions, should be reported regardless of the amount of the transactions; and, the CTRs should be reported for the transactions of rupees two million and above as per requirements of AML, Act.

(vi) The basis of deciding whether an STR is being filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

(vii) The employees of FEM are strictly prohibited to disclose the fact to the customer or any other quarter that a STR or related information is being or has been reported to any authority, except if required by law.

(viii) FEM without disclosing the contents of STRs, shall intimate to the Commission on bi-annual basis the number of STRs reported and FEM shall ensure that status report (indicating No. of STRs only) shall reach the AML Department within seven days of close of each half year. The CO should ensure prompt reporting in this regard

20)) SANCTION COMPLIANCE

FEM will not form business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

The individuals and entities designated under the UNSC resolutions are subject to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses. Such sanctions also extend to any funds, financial assets and economic resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

FEM will also require to screen our entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list

Where there is a true match or suspicion, we shall take steps that are required to comply with the sanctions obligations including immediately–

a. Freeze without delay the customer's fund or block the transaction, if it is an existing customer;
b. reject the customer, if the transaction has not commenced;
c. Lodge a STR with the FMU; and
d. Notify the SECP

21) EMPLOYEES TRAINING AND DUE DILIGENCE

Training

FEM will implemented a clear and well articulated staff training policy to ensure that relevant staff receive adequate AML/CFT training to maintain their AML/CFT knowledge and competence

FEM will ensure that all the appropriate staff, receive training on ML and TF prevention on a regular basis, all staff is fully conversant with procedures and its importance. Training will be provided once in a year or as and when required, or where there are changes in the relevant laws.

FEM will provide staff training in the recognition and treatment of suspicious activities. FEM will ensure that those who deal with the public, such as sales person, opening of new account and dealing with existing customers, should be aware of the need to verify the customer's identity.

FEM will provide AML/CFT training tor all your new staff, irrespective of their seniority and before joining.

Due Diligence

FEM will develop and implement a comprehensive employee due diligence policy and procedure to be implemented/ carried out at the time of hiring all employees permanent or contractual. This shall include but not limited to verification of antecedents and screening procedures to verify that person being inducted/ hired has a clean history.

22) COMPLIANCE OFFICER

A Compliance Officer is appointed at a management level, who shall report directly to the Chief Executive Officer and Company Secretary

A Compliance Officer has been designated who shall ensure that FEM is fully complied with the relevant provisions of AML / CFT Regulations, who shall ensure that the reporting of suspicious transaction is made and shall monitor, review and update the policies and procedure. He shall be the point of contact with the supervisory authorities. The officer will be responsible among other matters and issues for the following areas:

a) maintaining an effective AML / CFT compliance culture

b) the regulated person effective compliance with the relevant provisions of these Regulations, the AML Act, the Anti-Money Laundering Rules, 2008, the Anti-Money Laundering Regulations, 2015 and other directions and guidelines issued under the aforementioned regulations and laws, as amended from time to time conduct training for staff to identify suspicious activities
c) monitor, review and update the policies and procedure
d) timely report of the suspicious transactions
e) timely submission of accurate data
f) Other responsibilities as FEM may deem necessary in order to ensure compliance with the Regulations.
g) ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the regulated person and are effectively implemented;
h) timely submission of accurate data/ returns as required under the applicable laws;
i) monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
j) such other responsibilities as the regulated person may deem necessary in order to ensure compliance with these regulations.

23) INTERNAL AUDIT

FEM will on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures

The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

(a) Test the overall integrity and effectiveness of the AML/CFT systems and controls;

(b) assess the adequacy of internal policies and procedures in addressing identified risks, including;
- CDD measures
- Record keeping and retention
- Transaction monitoring;
-

(c) assess compliance with the relevant laws and regulations;
(d) test transactions in all areas of the RP, with emphasis on high–risk areas, products and services;
(e) assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
(f) assess the adequacy, accuracy and completeness of training programs;
(g) Assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts ;and
(h) Assess the adequacy of the RP's process of identifying suspicious activity including screening sanctions lists.

24) FINANCIAL GROUPS.-

Financial groups should implement group-wide programmes against ML/TF, which should be applicable, and appropriate to, all branches and majority-owned subsidiaries of the financial group and these should include the measures set out in in the Regulations and also-

1. policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;

2. the provision, at group-level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

3. adequate safeguards on the confidentiality and use of information exchanged

25) TIPPING-OFF

ii. The Law prohibits tipping-off. However, a risk exists that customers could be unintentionally tipped off when we seeking to complete our CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

iii. Therefore, if FEM form a suspicion of ML/TF while conducting CDD or ongoing CDD, FEM should take into account the risk of tipping-off when performing the CDD process.

iv. If FEM reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and should file a STR. FEM will ensure that its employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD

26 SANCTIONS COMPLIANCE- IMPLEMENTATION OF UN SECURITY COUNCIL RESOLUTIONS

FEM will not form business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997. The types of sanctions that may be imposed include:

i. targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly;

ii. economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;

iii. currency or exchange control;

iv. arms embargoes, which would normally encompass all types of military and paramilitary equipment;

v. prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;

vi. import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.;

vii. visa and travel bans and

viii. Targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of Weapons of Mass Destruction (WMD) and its financing.

27) RISK ASSESSMENT AND APPLYING A RISK BASED APPROACH

The SECP AML/CFT Regulations shift emphasis from one-size-fits-all approach to Risk Based Approach ('RBA'). In this respect, FEM will carryout ML/TF risk assessment and apply RBA to prevent or mitigate ML and TF.

The RBA enables FEM to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. FM will develop an appropriate RBA for particular organization, structure and business activities and apply the RBA on a group-wide basis, where appropriate.

As a part of the RBA, FEM will:

i) Identify ML/TF risks relevant to them;
ii) Assess ML/TF risks in relation to-
    a. Customers (including beneficial owners);
    b. Country or geographic area in which its customers reside or operate;
    c. Products, services and transactions; and
    d. Delivery channels.

iii) Design and implement policies, controls and procedures approved by its Board of Directors;
iv) Monitor and evaluate the implementation of mitigating controls;
v) Keep their risk assessments current through ongoing reviews;

vi) Document the RBA including implementation and monitoring procedures and updates to the RBA; and

vii) Have appropriate mechanisms to provide risk assessment information to the Commission.

Under the RBA, where there are higher risks, RPs are required to take enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures may be permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high-risk situations or situations which are outside the RP's risk tolerance, the RP may decide not to take on the accept the customer, or to exit from the relationship.

In view of the fact that the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Many of the CFT measures entities have in place will overlap with their AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison relationships with the authorities. The guidance provided in these guidelines, therefore, applies to CFT as it does to AML, even where it is not explicitly mentioned.

The process of ML/TF risk assessment has four stages:

a. Identifying the area of the business operations susceptible to ML/TF;
b. Conducting an analysis in order to assess the likelihood and impact of ML/TF;
c. Managing the risks; and
d. Regular monitoring and review of those risks.

28) ML/TF WARNING SIGNS/ RED FLAGS

The following are some of the warning signs or "red flags" which should be alerted. The list is not exhaustive, but includes the following:

Modaraba

a. Exposure secured by pledged assets held by third parties unrelated to the borrower.

b. Exposure secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.

c. Exposure are made for, or are paid on behalf of, a third party with no reasonable explanation.

d. To secure a Exposure, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via a currency or multiple monetary instruments.

e. Exposure that lack a legitimate business purpose, provide the bank with significant fees or assuming little or no risk, or tend to obscure the movement of funds (e.g.,

loans made to a borrower and immediately sold to an entity related to the borrower or back to back loans without any identifiable and legally admissible purpose).

Brokerage Houses

a) Client who are unknown to the broker and verification of identity / incorporation proves difficult;

b) Client who wish to deal on a large scale but are completely unknown to the broker;

c) Client who wish to invest or settle using cash;

d) Client who use a cheque that has been drawn on an account other than their own;

e) Client who change the settlement details at the last moment;

f) Client who insist on entering into financial commitments that appear to be considerably beyond their means;

g) Client who accept relatively uneconomic terms, when with a little effort they could have a much better deal;

h) Client who have no obvious reason for using the services of the broker (e.g.: Client with distant addresses who could find the same service nearer their home base;

i) Client who refuse to explain why they wish to make an investment that has no obvious purpose;

j) Client who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;

k) Client trades frequently, selling at a loss

l) Client who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;

m) Any transaction involving an undisclosed party;

n) Transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and

o) Significant variation in the pattern of investment without reasonable or acceptable explanation

p) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.

q) Transactions involve penny/microcap stocks.

r) Client requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.

s) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.

t) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.

u) Client invests in securities suddenly in large volumes, deviating from previous transactional activity.

v) Client conducts mirror trades.

w) Client Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.